VECTOR SPACES OVER A FINITE PSEUDO FIELD

by

LONNIE WILLIAMS KEITH

B. S., Johnson C. Smith University, 1964

A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1966

Approved by:

Leonard D. Fuller

Major Professor

TABLE OF CONTENTS

INTRODUCTION

The purpose of this report is to discuss vector spaces over a finite pseudo field. In order to do this, it is necessary that the properties of the finite pseudo field, $P/\{m\}$, be shown. In the process of establishing properties of this system, it will be seen why the system is referred to as a pseudo field.

Once the properties of the system, $P/\{m\}$, are known, a definition of a vector space over this system can be formulated. It will be found that many of the properties of the system are similar to the properties of the vector spaces over $P/\{m\}$.

Linear independence and linear dependence are discussed at great length because they are two important concepts in the study of vector spaces. Most of the discussion of linear independence is concerned with the following problems:

1. How is linear independence related to the unique representation of the zero vector.
2. How to find the number of linear combinations of a set of linearly independent vectors which represent a vector.
3. How to determine whether or not a given set of vectors is linearly independent.

ALGEBRAIC SYSTEM, $P/\{m\}$

The purpose of this section is to give properties of the system $P/\{m\}$ where P is the ring of integers and $m = p^k$. The integer p is prime in P and k is any positive integer. For

convenience the system $P/\{m\}$ will be denoted as Q.

The elements of the system Q can be expressed as polynomials over P. The general elements are of the form:

$$c = \sum_{i=0}^{k-1} c_i p^i \qquad\qquad d = \sum_{i=0}^{k-1} d_i p^i$$

The c_i belong to P such that $0 \leq c_i \leq p-1$. The c_i is referred to as the coefficient of p^i in the element. Since there are never more than k coefficients it is obvious that Q is finite.

The concept of degree is important in the discussion of the system Q.

Definition 1. The degree of an element c is the minimal index of the c_i that are nonzero. The degree of an element c is denoted as deg(c).

The element with all $c_i=0$ is the zero element. By Definition 1 the zero element does not have a degree thus it is convenient to say its degree is k. The familiar symbol, 0 is used to denote the zero element.

Definition 2. Two elements c and d are equal, where deg(c) $=r$ and $\deg(d)=s$, if and only if $r=s$ and $c_i=d_i$ for each i.

There are two binary operations in Q. They are the two familiar operations of addition and multiplication. The definition of the sum is as follows.

Definition 3. The sum c+d is defined as the element of Q formed by first adding corresponding coefficients of c and d. Then these coefficients whose sums are greater than or equal to pare reduced by p with 1 added to the next higher coefficient.

$$c+d = \sum_{i=0}^{k-1} c_i p^i + \sum_{i=0}^{k-1} d_i p^i = \sum_{i=0}^{k-1} (c_i+d_i)p^i$$

To find the degree of a sum of elements of Q, the following lemmas are needed.

Lemma 1. Let c and d be elements of Q. If deg(c)=r and deg(d)=s, $r < s$, then deg(c+d)=r.

Proof. Since deg(c)=r, $c_i=0$ for i=0,1,...,r-1. Since deg(d)=s then $d_i=0$ for i=0,1,...,s-1. Hence $c_i+d_i=0$ for i=0,1, ...,r-1 and since $r < s$, $c_r+d_r=c_r+0=c_r \neq 0$. Thus deg(c+d)=r.

Lemma 2. Let c and d be elements of Q. If deg(c)=r and deg(d)=s, r=s, the $r \leq \deg(c+d) \leq k$.

Proof. Since deg(c)=r and deg(d)=s, r=s, then $c_i=d_i=0$ for all i=0,1,...,r-1. Hence $c_i+d_i=0$ for i=0,1,...,r-1 so the degrees is at least r.

From this lemma it can be seen that the sum of two elements can be the zero element. This implies the possibility of the existence of an additive inverse.

The definition of the second binary operation in Q is

Definition 4. The product cd is defined as the element of Q obtained after simplifying the coefficients in the formal product.

$$cd = \left(\sum_{i=r}^{k-1} c_i p^i\right) \left(\sum_{j=s}^{k-1} d_j p^j\right) = \sum_{i=r}^{k-1} \sum_{j=s}^{k-1} c_i d_j \, p^{i+j}$$

When the coefficients in the formal product are greater than p then the coefficients are expressed as $\sum_{i=0} x_i p^i$ where x_1 is

added to the next coefficient. If the exponent of p is greater than or equal to k then the coefficient involving that p is equal to zero.

The lemma concerned with finding the degree of a product follows.

Lemma 3. Let c and d be elements of Q. If deg(c)=r and deg(d)=s then deg(cd)=r+s, if $r+s < k$. If $r+s \geq k$ then cd is the zero element.

Proof. The product $cd = \sum_{i=r}^{k-1} \sum_{j=s}^{k-1} c_i d_j p^{i+j}$.

Since deg(c)=r, $c_i=0$ for i=0,1,...,r-1 and deg(d)=s, $d_j=0$ for j=0,1,...,s-1, $c_i d_j=0$ for i+j=0,1,..., r+s-1. On the other hand $c_r d_s \neq 0$, hence the degree of cd is r+s if $r+s<k$. If $r+s \geq k$ then deg(cd)=k.

Theorem 1 can now be stated.

Theorem 1. Q is a commutative ring with unity.

Proof. (i) c+d = d+c.

By the definition of addition,

$$c+d = \sum_{i=0}^{k-1} c_i p^i + \sum_{i=0}^{k-1} d_i p^i = \sum_{i=0}^{k-1} (c_i + d_i) p^i.$$

Since P is the ring of integers, $(c_i+d_i) = (d_i+c_i)$. Therefore

$$\sum_{i=0}^{k-1} (c_i + d_i) p^i = \sum_{i=0}^{k-1} (d_i + c_i) p^i = \sum_{i=0}^{k-1} d_i p^i +$$

$$\sum_{i=0}^{k-1} c_i p^i = d+c.$$

(ii) $(b+c)+d = b+(c+d)$. By the definition of addition

$$\sum_{i=0}^{k-1} (b_i + c_i)\, p^i + \sum_{i=0}^{k-1} d_i p^i = \sum_{i=0}^{k-1} ((b_i + c_i) + d_i)\, p^i.$$

Since P is the ring of integers its elements are associative under addition. Thus

$$\sum_{i=0}^{k-1} ((b_i + c_i) + d_i)\, p^i = \sum_{i=0}^{k-1} (b_i + (c_i + d_i))\, p^i$$

which is equal to $\sum_{i=0}^{k-1} b_i p^i + \sum_{i=0}^{k-1} (c_i + d_i)\, p^i = b+(c+d)$ by the definition of addition.

(iii) $c+0=c$. By the definition of addition

$$c+0 = \sum_{i=0}^{k-1} c_i p^i + \sum_{i=0}^{k-1} 0 \cdot p^i = \sum_{i=0}^{k-1} (c_i + 0)\, p^i.$$

Because $c_i+0 = c_i$ in P,

$$\sum_{i=0}^{k-1} (c_i + 0)\, p^i = \sum_{i=0}^{k-1} c_i p^i = c.$$

(iv) The inverse of c under addition, c^*, is an element of Q such that $c^*+c = 0$. Suppose c has degree r then

$$c^* = c'_r\, p^r + \sum_{j=r+1}^{k-1} (c'_j - 1)\, p^j.$$

where c_i' is defined such that $c_i+c_i' = 0+1\cdot p$ in Q. Thus

$$\sum_{i=r}^{k-1} c_i p^i + (c_r' p^r + \sum_{j=r+1}^{k-1} (c_j' - 1)\, p^j)$$

$$= (c_r + c_r')\, p^r + \sum_{j=r+1}^{k-1} (c_j + c_j' - 1)\, p^j.$$

By the definition of c_i' this is the zero element.

(v) cd=dc. By the definition of multiplication

$$cd = (\sum_{i=r}^{k-1} c_i p^i)(\sum_{j=s}^{k-1} d_j p^j) = \sum_{i=r}^{k-1} \sum_{j=s}^{k-1} c_i d_j\, p^{i+j}.$$

Since P is the ring of integers multiplication and addition are commutative and the distributive property holds. Therefore

$$\sum_{i=r}^{k-1} \sum_{j=s}^{k-1} c_i d_j\, p^{i+j} = \sum_{j=s}^{k-1} \sum_{i=r}^{k-1} d_j c_i\, p^{j+i} = (\sum_{j=s}^{k-1} d_j p^j)$$

$$(\sum_{i=r}^{k-1} c_i p^i) = dc$$

(vi) (bc)d = b(cd). By the definition of multiplication if deg(b)=t then

$$(bc)d = (\sum_{h=t}^{k-1} \sum_{i=r}^{k-1} b_h c_i\, p^{h+i})(\sum_{j=s}^{k-1} d_j p^j) =$$

$$\sum_{h=t}^{k-1}\sum_{i=r}^{k-1}\sum_{j=s}^{k-1}(b_h c_i)d_j\, p^{h+i+j}.$$

Since P is the ring of integers its elements are associative with respect to multiplication. Therefore

$$\sum_{h=t}^{k-1}\sum_{i=r}^{k-1}\sum_{j=s}^{k-1}(b_h c_i)d_j\, p^{h+i+j} = \sum_{h=t}^{k-1}\sum_{i=r}^{k-1}\sum_{j=s}^{k-1} b_h(c_i d_j)\, p^{h+i+j}$$

which is equal to $(\sum_{h=t}^{k-1} b_h p^h)(\sum_{i=r}^{k-1}\sum_{j=s}^{k-1} c_i d_j\, p^{i+j}) = b(cd)$ by the definition of multiplication.

(vii) The unit element, I is an element of Q such that bI =b. Let

$$I = 1 + \sum_{i=0}^{k-1} 0\cdot p^i$$

where 1 is the unit element of P. The unit element has degree zero and can be written simply as 1. Therefore

$$bI = (\sum_{h=t}^{k-1} b_h p^h)I = (\sum_{h=t}^{k-1} b_h p^h)(1) = \sum_{h=t}^{k-1}(1)b_h p^h = \sum_{h=t}^{k-1} b_h p^h = b$$

by the property of the unit element of P.

(viii) b(c+d)=bc+bd. By the definition of addition and multiplication

$$b(c+d) = (\sum_{h=t}^{k-1} b_h p^h)(\sum_{i=0}^{k-1}(c_i + d_i)\, p^i) = \sum_{h=t}^{k-1}\sum_{i=0}^{k-1} b_h(c_i+d_i)p^{h+i}.$$

Since P is the ring of integers its elements possess the distributive property, thus

$$\sum_{h=t}^{k-1} \sum_{i=0}^{k-1} b_h(c_i + d_i)\, p^{h+i} = \sum_{h=t}^{k-1} \sum_{i=0}^{k-1} (b_h c_i + b_h d_i)\, p^{h+i}.$$

By the definition of addition

$$\sum_{h=t}^{k-1} \sum_{i=0}^{k-1} (b_h c_i + b_h d_i)\, p^{h+i} = \sum_{h=t}^{k-1} \sum_{i=0}^{k-1} b_h c_i\, p^{h+i}$$

$$+ \sum_{h=t}^{k-1} \sum_{i=0}^{k-1} b_h d_i\, p^{h+i} = bc + bd.$$

Since Q is a commutative ring is it also a field? The answer is no. By Lemma 3 there are proper divisors of zero in the system.

Two properties of Q are now discussed.

Lemma 4. If $cd=0$, $d\neq 0$ then c has degree greater than zero.

Proof. From Lemma 3 it is seen that if $\deg(c)=r$ and $\deg(d)=s$ then the product $cd=0$ if $r+s \geq k$. Hence $s \geq k-r$. If $r=0$ then $s \geq k$. This contradicts the fact that $d\neq 0$.

The degree of the unit element, I in Q is zero. Let a be a nonzero element in Q. If $\deg(a)=u>0$, suppose there is an element of Q, a^{-1}, such that $aa^{-1} = a^{-1}a = I$. If $\deg(a^{-1})=v$ then $\deg(aa^{-1})=u+v$. By the definition of degree $v \geq 0$ hence $u+v>0$. Thus no multiplicative inverse exists for nonzero elements of Q with degree greater than zero.

A field is defined as a commutative ring with unity having

the property that every nonzero element of the field has a multiplicative inverse. Thus Q is certainly not a field. This is why Q is referred to as a pseudo field.

VECTOR SPACES

Definition and Properties

Vectors can be defined as a special type of matrices which have only one column or one row. The general definition of a vector space is given.

Definition 5. A vector space $V_n(F)$ consists of a field F with elements c and a nonempty set V with elements $A=[a_1,a_2 \ldots a_i \ldots]$, where $a_i \in F$ such that:

(i) there is an operation of addition defined on V such that V forms a commutative group.

(ii) there is an operation of scalar multiplication cA defined for all $c \in F$ and all $A \in V$ with the following properties,

(a) $1A = A$, 1 is the unity of F

(b) $(c_1 + c_2) A = c_1A + c_2A$

(c) $c_1(c_2A) = (c_1c_2)A$

(d) $c(A_1 + A_2) = cA_1 + cA_2$

Let F be the finite pseudo field Q. The elements of $V_n(Q)$ are of the form $A_i=[a_{i1}a_{i2}\ldots a_{in}]$ where $a_{ij} \in Q$, $j=1,2,\ldots,n$. Theorem 2 follows.

Theorem 2. The set of all vectors of the form $A=[a_1a_2\ldots a_n]$ over Q is a finite vector space $V_n(Q)$.

Proof. The sum of two vectors A+B is defined as the vector over Q whose components are the sums of the two corresponding components of A and B. Hence

$$A + B = [a_1 a_2 \ldots a_n] + [b_1 b_2 \ldots b_n] = [a_1+b_1 \; a_2+b_2 \ldots a_n+b_n].$$

Since Q is a commutative ring and $(a_i+b_i) \in Q$ then $(a_i+b_i) = (b_i+a_i)$. Therefore

$$[a_1+b_1 \; a_2+b_2 \ldots a_n+b_n] = [b_1+a_1 \; b_2+a_2 \ldots b_n+a_n]$$

which is B+A by the definition of addition in $V_n(Q)$.

If $A,B,C, \in V_n(Q)$ then $(A+B)+C = A + (B+C)$. By the definition of addition in $V_n(Q)$

$$[a_1+b_1 \; a_2+b_2 \ldots a_n+b_n] + [c_1 \; c_2 \ldots c_n] =$$

$$[((a_1+b_1)+c_1) \; ((a_2+b_2)+c_2) \ldots ((a_n+b_n)+c_n)].$$

Since Q is a commutative ring its elements are associative. Thus

$$[((a_1+b_1)+c_1) \; ((a_2+b_2)+c_2) \ldots ((a_n+b_n)+c_n)] =$$

$$[(a_1+(b_1+c_1)) \; (a_2+(b_2+c_2)) \ldots (a_n+(b_n+c_n))]$$

which is equal to A+(B+C) by the definition of addition.

The identity vector of addition is the vector with all of its components zero and is denoted as Z. For any vector A the vector Z has the property that A+Z=A.

For each vector $A=[a_1 a_2 \ldots a_n]$ there exists a vector $A^*=[a^*_1 \; a^*_2 \ldots a^*_n]$ where $a^*_i+a_i=0$, such that $A+A^*=Z$. This is the additive inverse of A. Therefore $V_n(Q)$ forms a commutative

group.

For all c or d that belong to Q and $A_1 \in V$, scalar multiplication is defined in the following way:

$$cA = [ca_1 \ ca_2 \ \dots \ ca_n].$$

The properties of scalar multiplication hold in $V_n(Q)$.

(a) IA=A, I is the unity of Q. By the definition of scalar multiplication

$$IA = [Ia_1 \ Ia_2 \ \dots \ Ia_n].$$

Since I is the unity of Q then $Ia_1=a_1$, hence

$$IA = [Ia_1 \ Ia_2 \ \dots \ Ia_n] = [a_1 \ a_2 \ \dots \ a_n] = A.$$

(b) (c+d)A = cA+dA. By the definition of scalar multiplication

$$(c+d)\ [a_1 \ a_2 \ \dots a_n] = [(c+d)a_1 \ (c+d)a_2 \ \dots \ (c+d)\ a_n].$$

Since Q is a commutative ring the distributive property holds. Therefore

$$[(c+d)a_1 \ (c+d)a_2 \ \dots \ (c+d)a_n] = [(ca_1+da_1) \ (ca_2+da_2) \ \dots \ (ca_n+da_n)]$$

which is cA+dA by the definition of addition.

(c) c(dA) = (cd)A. Thus by definition of scalar multiplication

$$c(dA) = [c(da_1) \ c(da_2) \ \dots \ c(da_n)].$$

Since Q is a commutative ring its elements are associative.

Therefore,

$$\left[c(da_1)\ c(da_2)\ \ldots\ c(da_n)\right] = \left[(cd)a_1\ (cd)a_2\ \ldots\ (cd)a_n\right]$$

which is (cd)A by the definition of scalar multiplication.

(d) $c(A_1+A_2) = cA_1+cA_2$, thus by the definition of scalar multiplication

$$c(A_1 + A_2) = \left[c(a_{11} + a_{21})\ c(a_{12} + a_{22})\ \ldots\ c(a_{1n} + a_{2n})\right].$$

Since Q is a commutative ring the distributive property holds. Therefore

$$\left[c(a_{11} + a_{21})\ c(a_{12} + a_{22})\ \ldots\ c(a_{1n} + a_{2n})\right] =$$

$$\left[(ca_{11} + ca_{21})\ (ca_{12} + ca_{22})\ \ldots\ (ca_{1n} + ca_{2n})\right] = cA_1 + cA_2.$$

Different symbols for the zero vector and the zero element of Q have been used. Henceforth the symbol for the zero element of Q will also be used for the symbol of the zero vector.

The following definition aids in identifying subspaces of given vector spaces.

Definition 6. A nonempty subset U of $V_n(Q)$ is a subspace of $V_n(Q)$ if U is a vector space over Q.

By Definition 6 it can be proved that U is a subspace of $V_n(Q)$ if U is closed under addition and scalar multiplication.

The definition of a vector space implies that if A_1 and A_2 belong to $V_n(Q)$ then A_1+A_2 belong to $V_n(Q)$. The vectors cA_1 and dA_2 belong to $V_n(Q)$ for all $c,d \in Q$, hence cA_1+dA_2 also belong to $V_n(Q)$. The next definition is a generalization of this concept.

Definition 7. A linear combination of a set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is the vector, $\sum_{i=1}^{t} c_i A_i$ where $c_i \in Q$.

It is now easily verified that the set of all linear combinations of a set of vectors, $\{A_1, A_2, \ldots, A_t\}$ of $V_n(Q)$ is a subspace of $V_n(Q)$.

Let W be the set of all linear combinations of the set of vectors. If B and C are elements of W, then

$$B = \sum_{i=1}^{t} b_i A_i \text{ and } C = \sum_{i=1}^{t} c_i A_i$$

where b_i and c_i belong to Q. Then

$$B + C = \sum_{i=1}^{t} b_i A_i + \sum_{i=1}^{t} c_i A_i = \sum_{i=1}^{t} (b_i A_i + c_i A_i).$$

By the property (b) of scalar multiplication,

$$\sum_{i=1}^{t} (b_i A_i + c_i A_i) = \sum_{i=1}^{t} (b_i + c_i) A_i.$$

Thus B + C is a linear combination of the set of vectors, $\{A_1, A_2, \ldots, A_t\}$ and therefore an element of W. Closure under addition has been shown. If $d \in Q$ then

$$dB = d \sum_{i=1}^{t} b_i A_i = \sum_{i=1}^{t} d(b_i A_i).$$

By the property (c) of scalar multiplication,

$$\sum_{i=1}^{t} d(b_i A_i) = \sum_{i=1}^{t} (db_i) A_i.$$

Therefore dB belongs to W and closure under scalar multiplication has been shown. Thus W is a subspace of $V_n(Q)$ since it is a nonempty subset of $V_n(Q)$ and it is closed under addition and scalar multiplication.

For a linear combination of any set of vectors the zero vector can be obtained. The next section will consider this.

Linear Dependence and Linear Independence

In a vector space $V_n(F)$ the trivial linear combination is the linear combination where all the scalars are zero. The set of vectors is said to be linearly independent if the zero vector is given only by the trivial combination of the set, otherwise the set is linearly dependent.

For the system $V_n(Q)$ a change has to be made in the definitions of linear independence and linear dependence.

Definition 7. A set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is linearly independent if $\sum_{i=1}^{t} c_i A_i = 0$, implies that all c_i have degree greater than zero. Vectors which are not linearly independent are linearly dependent.

Definition 8. A set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is linearly dependent if $\sum_{i=1}^{t} c_i A_i = 0$, implies that at least one c_i can have degree zero.

Fundamental properties of linear dependence and linear independence are given in the following lemmas.

Lemma 5. The set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is linearly dependent if at least one of the vectors of the set is the zero vector.

Proof. Let A_1 be the zero vector. By property (a) of scalar multiplication in $V_n(Q)$ $IA_1 = A_1 = 0$, thus $(IA_1 + \sum_{i=2}^{k-1} 0 \cdot A_i) = 0$. Since the scalar for A_1 is of degree zero, the set is linearly dependent.

Lemma 6. The set $\{A\}$ consisting of one vector is linearly independent if $A \neq Z$.

Proof. Since $A \neq Z$, then $cA = [ca_1 ca_2 \ldots ca_n] = 0$ if and only if the scalar c has degree greater than zero by Lemma 4. Hence, the set is linearly independent by definition.

Lemma 7. If the set $\{A_1, A_2, \ldots, A_t\}$ is linearly independent then any nonempty subset of this set is linearly independent.

Proof. Consider a subset, $\{A_1, A_2, \ldots, A_h\}$ where $1 \leq h < t$ and $\sum_{i=1}^{h} c_i A_i = 0$. Then

$$(\sum_{i=1}^{h} c_i A_i + \sum_{i=h+1}^{t} 0 \cdot A_i) = 0.$$

Since the set $A_1, A_2, \ldots, A_t$ is linearly independent, it follows that all c_i have degree greater than zero. Thus c_i where $i = 1,2,\ldots,h$ must have degree greater than zero. Hence $A_1, A_2, \ldots, A_h$ is a linearly independent subset.

Lemma 8. A set of vectors, $A_1, A_2, \ldots, A_t$ containing a linearly dependent set is linearly dependent.

Proof. Let $\{A_1, A_2, \ldots, A_m\}$ be the linearly dependent subset where $1 \leq m < t$. Thus $\sum_{i=1}^{m} c_i A_i = 0$ implies that at least one c_i has degree zero. Obviously

$$\left(\sum_{i=1}^{m} c_i A_i + \sum_{i=m+1}^{t} 0 \cdot A_i\right) = 0.$$

Thus the set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is linearly dependent by definition.

If U is the set of all linear combinations of a set of vectors, $\{A_1, A_2, \ldots, A_t\}$ of $V_n(Q)$, and the set of vectors, $\{A_1, A_2, \ldots, A_t\}$ is linearly independent, then is each vector of U uniquely expressible as a linear combination of the vectors $A_1, A_2, \ldots, A_t$? An answer to this question is illustrated in Example 1 by considering the basic question, is the zero vector uniquely expressible as a linear combination of the vectors $A_1, A_2, \ldots, A_t$?

Example 1. Consider the subset U of $V_2(Q)$, where k=3, spanned by the vector $\left[p\ p^2\right]$. A scalar multiple of this vector would be of the form

$$a\left[p\ p^2\right] = (a_o + a_1 p + a_2 p^2)\left[p\ p^2\right] = \left[a_o p + a_1 p^2\ a_o p^2\right].$$

If this were the zero vector then $a_o = a_1 = 0$. Yet a_2 can have any one of p values; thus there are p expressions for the zero vector. If

$$a\left[p\ p^2\right] = b\left[p\ p^2\right] \text{ then } \left[a_o p + a_1 p^2\ a_o p^2\right] = \left[b_o p + b_1 p^2\ b_o p\right].$$

This implies that $a_0=b_0$, $a_1=b_1$ but b_2 does not have to equal a_2. Thus linear independence does not imply unique representation of a vector.

Example 1 implies that each vector of U cannot be represented uniquely as a multiple of a linearly independent vector. Thus if a set of linearly independent vectors is given, then how many linear combinations of these vectors can represent a given vector of U? In order to answer this question the concept of the degree of a vector is needed.

Definition 9. The degree of a vector is the minimal degree of the components of the vector.

To find the degree of a scalar multiple of a vector the following lemma is given.

Lemma 9. If A is a vector of degree u and deg(c)=v, then cA is a vector with degree u+v. The case where $u+v \geq k$ can occur when A=0, c=0 or when both A and c are of degree greater than zero.

Proof. By the definition of scalar multiplication

$$cA = [ca_1\ ca_2\ \ldots\ ca_n].$$

Let a_n be one of the components of A with degree u. By Lemma 3 $\deg(ca_n)=u+v$. If $u+v \geq k$ then by Lemma 4 c=0, $a_n=0$ or both c and a_n are of degree greater than zero.

It is now possible to prove the following theorem.

Theorem 3. If the single nonzero vector, A, has degree u then the number of possible expressions for the vector dA is p^u.

Proof. Any multiple of a vector dA can be written as (c+d)A

where cA=0. Therefore all representations for dA are obtained by adding each representation for cA=0 to dA (this set includes, when c=0, the multiple d).

The zero vector has degree k, hence by Lemma 9 if the vector cA=0 then c is of degree at least k-u.

Let A be of degree zero then c has degree at least k. Thus c is the zero element and there is only one representation for any vector cA.

Let A be of degree one then c has degree at least k-1. There is only one possible nonzero coefficient of c. Hence c can be any of p values. Thus there are p representations for any vector cA.

Let A be of degree two then c has degree at least k-2. There are two possible nonzero coefficients of c. Each coefficient can assume any one of p values. Since c can be anyone of p^2 values, there are p^2 representations for cA.

Thus by induction if c is of degree at least k-u then there are u possible nonzero coefficients of c that can be anyone of p values. Since c can assume p^u values, the vector cA can be expressed in p^u ways.

The following corollary is a special case of Theorem 3 and a proof will not be given.

Corollary 1. For a single vector A with degree zero each multiple of A is uniquely expressible.

The next theorem considers a set of more than one vector.

Theorem 4. If vectors $A_1, A_2, \ldots, A_t$ have degrees $u_1, u_2,$

$\ldots, u_t$ respectively, then the number of possible expressions for the vector

$$\sum_{i=1}^{t} c_i A_i \quad \text{is} \quad \prod_{i=1}^{t} p^{u_i}.$$

Proof. By Theorem 3 for each i there are p^{u_i} ways of expressing $c_i A_i$. For each pair i and j there are $p^{u_i}\, p^{u_j}$ ways of expressing $c_i A_i + c_j A_j$. Thus by inductive reasoning it is obvious that the number of expressions for

$$\sum_{i=1}^{t} c_i A_i \quad \text{is} \quad \prod_{i=1}^{t} p^{u_i}.$$

The next paragraphs consider the question of determining whether a given set of vectors is linearly independent.

Example 2. Consider the subspace of $V_3(Q)$, where k=3, spanned by the set of two vectors, $[p^2\ p\ 1]$, $[p\ p\ p^2]$. If

$$a_1 [p^2\ p\ 1] + a_2 [p\ p\ p^2]$$

$$= (a_{10} + a_{11}p + a_{12}p^2)[p^2\ p\ 1] + (a_{20} + a_{21}p + a_{22}p^2)[p\ p\ p^2]$$

$$= [a_{10}p^2\ a_{10}p\ a_{10} + a_{11}p^2\ a_{10} + a_{11}p + a_{12}p^2] + [a_{20}p + a_{21}p^2\ a_{20}p + a_{21}p^2\ a_{20}p^2]$$

$$= [a_{20}p + (a_{10} + a_{21})p^2\ (a_{10} + a_{20})p + (a_{11} + a_{21})p^2\ a_{10} + a_{11}p + (a_{12} + a_{20})p^2]$$

is the zero vector then

$$a_{20} = 0 \qquad a_{10} + a_{20} = 0 \qquad a_{10} = 0 \qquad a_{10} + a_{21} = 0$$

$$a_{11} + a_{21} = 0 \qquad a_{11} = 0 \qquad a_{12} + a_{20} = 0.$$

Since a_{10} and a_{20} are equal to zero the deg(a_1) and deg(a_2) are greater than zero. Thus the set is linearly independent.

The number of unknowns and equations required from this set can be determined as follows. The vectors can be used to form a matrix

$$\begin{bmatrix} p^2 & p & 1 \\ p & p & p^2 \end{bmatrix}.$$

The degree of each row is zero and one respectively; hence there would be three unknowns to determine for a_1 and two for a_2. The degree of each column vector is one, one and zero respectively. Thus the number of equations determined for each component is two, two and three.

The general case and explanation of Example 2 follows.

Consider a set of m vectors $\{A_1, A_2, \ldots, A_m\}$, each with n components. If $\sum c_i A_i = 0$ then the number of unknowns are determined as follows.

The vectors are used to form a matrix

$$\begin{bmatrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{bmatrix}.$$

The degree of the row vector determines the number of unknowns involved for each vector. Each scalar has k coefficients so if the vector A_i has degree u_i then scalar c_i has k-u_i coefficients

that need to be determined. Hence there are $mk-\sum u_i$ unknowns. The maximum number of unknowns possible is mk. The degree of each column vector determines the number of equations for each component. If the degree of the j^{th} column vector is u_j then there are $k-u_j$ equations for this component. Hence there are $nk-\sum u_j$ possible equations. The maximum number of equations possible is nk.

If given a set of m vectors such that each vector has n components, $m \leq n$, then the set is not necessarily linearly independent. If one of the m vectors is a multiple of another vector then the set is linearly dependent, because there are more unknowns than equations.

If given a set of m vectors such that each vector has n components, $m > n$, then the set is always linearly dependent. Since there are more unknowns than equations. Some of the unknowns are solved in terms of an arbitrary set of values for the remaining unknowns. Thus the unknowns are dependent upon each other in order to obtain the zero vector. Since each unknown can only assume p values there is a finite number of solutions. There is always the solution with all scalars $a_i=0$.

CONCLUSION

The elements of a vector space are usually from a field. In this report it has been shown what occurs in vector spaces when the elements are not from a field but from a given finite pseudo field. The properties of the elements of the finite

pseudo field, Q, affect the operations defined on the vector spaces and the properties of the vector spaces. The basic concepts involving vector spaces over Q have been discussed although there are concepts which were not covered in this paper.

ACKNOWLEDGMENT

The writer wishes to express her eternal gratitude to Dr. Leonard E. Fuller for his understanding, patient supervision, and helpful suggestions during the preparation of this report.

REFERENCES

Ayers, Frank Jr. Theory and Problems of Matrices. New York: Shaum Publishing Co., 1962.

Fuller, Leonard E. Basic Matrix Theory. Englewood Cliffs, New Jersey: Prentice-Hall, Inc., 1962.

McCoy, Neal H. Introduction to Modern Algebra. Boston: Allyn and Bacon, Inc., 1960.

Weiss, Marie J. Higher Algebra for the Undergraduate. New York: John Wiley & Sons, Inc., 1962.

VECTOR SPACES OVER A FINITE PSEUDO FIELD

by

LONNIE WILLIAMS KEITH

B. S., Johnson C. Smith University, 1964

AN ABSTRACT OF A MASTER'S REPORT

submitted in partial fulfillment of the

requirements for the degree

MASTER OF SCIENCE

Department of Mathematics

KANSAS STATE UNIVERSITY
Manhattan, Kansas

1966

The study of vector spaces over a given finite pseudo field, Q is considered in this report. In order to study the vector spaces, Q is defined and operations defined in Q are stated. The concept of the degree of elements in Q is defined. Lemmas concerned with the degree of a sum and the degree of a product in Q are proved.

The general definition of vector spaces over a field is given. Vectors with components belonging to Q are considered. Since all the properties of a vector space are satisfied, it is easily verified that the vectors over Q form a vector space which is denoted as $V_n(Q)$. Subspaces of $V_n(Q)$ are defined. The concept of linear combination is defined and it is shown that all linear combinations of $V_n(Q)$ form a subspace of $V_n(Q)$.

The concepts of linear dependence and independence are used in answering the question, what type of linear combination of nonzero vectors results in the zero vector? Linear dependence and linear independence are defined. Properties of linear dependence and linear independence are verified by lemmas. An example is presented to illustrate that linear independence does not imply unique representation of the zero vector. The concept of the degree of vectors in $V_n(Q)$ is defined. This concept is used to prove that the number of linear combinations for any particular vector can be found, if given a set of linearly independent vectors. A problem then arises of determining whether a given set of vectors is linearly dependent or independent. Another example is presented which hints at the solution of the problem. Linear

dependence or independence depends on the number of vectors in a set, the number of components in each vector, and the components themselves.